BRIAN M. BOYNTON, Principal Deputy Assistant Attorney General
BURDEN H. WALKER, Acting Deputy Assistant Attorney General

AMANDA N. LISKAMM, Director
LISA K. HSIAO, Senior Deputy Director
ZACHARY A. DIETERT, Assistant Director

CAMERON A. BROWN, Trial Attorney
JAMES T. NELSON, Senior Trial Attorney
AMANDA K. KELLY, Trial Attorney
U.S. Department of Justice
Consumer Protection Branch
Civil Division
450 5th Street, N.W.
Washington, D.C. 20001
Telephone: (202) 514-9471
Cameron.A.Brown@usdoj.gov

ISMAIL J. RAMSEY (CABN 189820)
United States Attorney
MICHELLE LO (NYRN 4325163)
Chief, Civil Division
VIVIAN F. WANG (CABN 277577)
Assistant United States Attorney
United States Attorney's Office
Northern District of California
450 Golden Gate Ave.
San Francisco, CA 94102
Telephone: (415) 436-7431
vivian.wang@usdoj.gov

Attorneys for Plaintiff United States of America

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. VERKADA INC., a corporation, Defendant.	Case No.: **COMPLAINT FOR PERMANENT INJUNCTION, CIVIL PENALTY JUDGMENT, AND OTHER EQUITABLE RELIEF**

Plaintiff, the United States of America, acting upon notification and referral from the Federal Trade Commission ("FTC" or "Commission"), for its Complaint alleges:

1. Plaintiff brings this action for Defendant's violations of Section 5(a) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a), and Section 7(a) of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act"), 15 U.S.C. § 7706(a). For these violations, Plaintiff seeks relief, including a permanent injunction, civil penalties, and other relief, pursuant to Sections 5(m)(1)(A) and 13(b) of the FTC Act, 15 U.S.C. §§ 45(m)(1)(A), 53(b), and the CAN-SPAM Act, 15 U.S.C. §§ 7701-7713.

SUMMARY OF CASE

2. Defendant has developed, advertised, and sold security cameras and other surveillance products to businesses (hereinafter "customers"). Defendant's customers include schools and medical facilities. Defendant's surveillance products captured and recorded individuals (hereinafter "consumers") in various, potentially sensitive, locations.

3. Defendant failed to use appropriate information security practices to protect customers' and consumers' personal information collected through the company's security cameras. These failures allowed a threat actor to access Defendant's customer support accounts, view customer cameras, and access personal information relating to customers and consumers, as described in greater detail below.

4. Defendant has publicly claimed both HIPAA certification or compliance and Privacy Shield compliance. However, such representations were deceptive as Defendant failed to provide reasonable or appropriate security for the personal information that it collected and maintained about customers and consumers.

5. Defendant was aware that, on multiple occasions, Defendant's employees and a venture capital investor posted positive ratings and reviews of Defendant and its products online but failed to disclose their association or current employment status with Defendant.

6. Defendant delivered a barrage of commercial emails that failed to include unsubscribe links or a clear opportunity to opt-out, failed to honor requests to opt out, and failed to include a valid physical postal address in commercial emails.

7. The above-referenced conduct constitutes multiple violations of the FTC Act and the CAN-SPAM Act.

JURISDICTION, VENUE, AND DIVISIONAL ASSIGNMENT

8. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), 1345, and 1355.

9. Venue is proper in this District under 28 U.S.C. §§ 1391(b)(1), (b)(2), (c)(2), and (d), 1395(a), and 15 U.S.C. § 53(b).

10. Divisional Assignment: Assignment to the San Francisco/Oakland Division is proper under Civil Local Rule 3-2(c) because Defendant has its principal place of business in San Mateo County and a substantial part of the events or omissions that give rise to the claims occurred there.

PLAINTIFF

11. Plaintiff brings this action upon notification and referral to the Attorney General by the FTC, pursuant to Section 16(a)(1) of the FTC Act, 15 U.S.C. § 56(a)(1). The FTC is an independent agency of the United States Government created by the FTC Act. 15 U.S.C. §§ 41-58. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC also enforces the CAN-SPAM Act, 15 U.S.C. §§ 7701-7713.

DEFENDANT

12. Defendant Verkada Inc. ("Verkada") is a Delaware corporation with its principal place of business at 405 E. 4th Ave., San Mateo, CA 94401. Verkada transacts or has transacted business in this District and throughout the United States.

COMMERCE

13. At all times relevant to this Complaint, Defendant has maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

DEFENDANT'S BUSINESS PRACTICES

14. Defendant is a cloud-based building security company that sells security cameras and other physical security products to over 12,000 businesses throughout the U.S. and abroad. Defendant's

customers span multiple industries, including education, government, healthcare, and hospitality. Approximately 80% of Defendant's security camera and building access control customers are businesses with 500 or fewer employees.

15. Defendant earned revenues of approximately $37 million in 2019, $90 million in 2020, and $73 million for the first two quarters of 2021.

16. Defendant's primary product sales are IP-enabled security cameras that store customers' data and archived video footage using Amazon Web Services' ("AWS") cloud-based storage. Defendant considers its security cameras to be "plug-and-play," meaning they require little set-up or configuration on the customer's end. Defendant's security cameras connect to Defendant's "Command" platform, a web-based platform which enables customers remote access to their security cameras, among other capabilities such as configuring security camera settings and viewing stored archive video footage. Between 2019 and 2021, Defendant sold more than 240,000 security cameras.

17. Through its customers, Defendant collects and maintains a variety of customers' and consumers' personal or sensitive information. Defendant's security cameras collect metadata about security camera usage, including IP addresses and locations of cameras. Defendant also collects and maintains a variety of other customer information, including names, physical addresses, customer usernames and password hashes, customers' site floorplans, names and titles of organization contacts, and customer Wi-Fi credentials.

18. With respect to consumers, Defendant's security cameras collect video footage from cameras, which may include captures of consumers and of other potentially sensitive personal information regarding consumers (e.g., visible medical records). Some video footage is collected from sensitive locations, including hospitals and elementary schools. Many such captures of consumers are inherently sensitive as one's presence in a particular location necessarily reveals one's personal information (e.g., a consumer captured in a psychiatric hospital strongly suggests that said consumer is seeking mental health services).

19. In addition to live surveillance capabilities, Defendant's security cameras include "People Analytics" features that allow customers to view high resolution images of all consumers whose

likenesses have either been recorded by their security cameras or uploaded to the Command platform, filter collected images by gender or clothing color, and search images through facial recognition or face-matching technology.

DEFENDANT'S INFORMATION SECURITY FAILURES

20. Defendant has engaged in multiple practices that, taken individually or together, failed to provide reasonable or appropriate security for the personal information that it collected and maintained from and about customers and consumers. Among other things, Defendant failed to:

a. Impose reasonable access management controls such as:

   i. requiring unique and complex passwords (i.e., long passwords not used by the individual for any other online service);

   ii. enforcing role-based access controls to safeguard personal information, such as implementing the principle of least privilege and requiring multi-factor authentication for account access across all of Defendant's systems;

   iii. issuing alerts for activities, such as unsuccessful logins to administrative accounts and the addition or removal of any account with administrative privileges;

b. Prevent data loss by establishing data protection controls, such as:

   i. performing data discovery and categorization for all sensitive personal information to ensure it is appropriately protected during transmission and storage;

   ii. implementing a data loss prevention solution that monitors for suspicious activities such as unauthorized data access and exfiltration; and

   iii. performing regular assessments to determine the effectiveness of protection measures;

c. Implement centralized logging and alerting capabilities;

d. Develop adequate security vulnerability management standards, policies, procedures, and practices, such as:

i. testing, auditing, assessing, or reviewing its products' or applications' security features; and

ii. conducting regular risk assessments, vulnerability scans, and penetration testing of its networks and databases;

e. Implement secure network controls, such as disabling unnecessary ports, protocols, and services, and properly configuring firewall settings;

f. Adequately encrypt customer's data in transit or at rest; and

g. Develop adequate written information security standards, policies, procedures, and practices; assess or enforce compliance with the written standards, policies, procedures, and practices that it did have; and implement training for employees (including engineers) regarding such standards, policies, procedures, and practices.

DEFENDANT'S INFORMATION SECURITY FAILURES LED TO MULTIPLE SECURITY INTRUSIONS

21. Defendant's failure to provide reasonable and appropriate security for the personal information it collected from and about customers and consumers led to the exposure, and the repeated risk of exposure, of that information.

22. In December 2020, a threat actor leveraged a security flaw in a legacy firmware build server after an employee failed to restore the original security settings for the server. The threat actor installed the "Mirai" malware onto the server and performed malicious activity, including weaponizing the server to launch denial-of-service attacks against other third-party internet addresses. Defendant was not aware that the server was compromised until AWS security flagged the activity more than two weeks later.

23. Subsequently, the cybersecurity and forensics firm that analyzed the December 2020 Mirai malware incident flagged "several security gaps" that Defendant needed to address, such as misconfigured servers, weak authentication and access management, and the lack of centralized logging and alerting capabilities. Moreover, due to Defendant's logging failures, the firm was unable to determine affirmatively if the threat actor had accessed or exfiltrated any data residing on the server. To

properly address the security gaps, the firm recommended, among other things, that Defendant: (a) rebuild the compromised legacy firmware build server from scratch, (b) upgrade authentication practices, (c) rotate credentials, (d) document an internal incident response plan, (e) eliminate account sharing, and (f) improve data security incident detection and alert practices. Accordingly, Defendant should have taken appropriate steps to improve Defendant's information security practices.

24. Defendant engaged a third-party cybersecurity consulting firm to conduct an enterprise-wide security posture assessment. The cybersecurity consulting firm shared the results of this assessment with Defendant in February 2021. Among other things, the cybersecurity consulting firm identified several critical and high level security gaps, including with respect to: (a) account monitoring; (b) administrative privileges; (c) data protection; (d) inventory of hardware and software assets; (e) security monitoring and logging; (f) secure network configurations; and (g) vulnerability management.

25. However, Defendant failed to address known security gaps and, on March 8, 2021, another threat actor gained access to one of Defendant's support level accounts that had administrative-level privileges (or "Super Admin" privileges). The threat actor gained Super Admin privileges by leveraging a security vulnerability in Defendant's customer support server. This breach occurred as a direct result of Defendant's failure to take proper precautions during a scheduled server update and allowed the intruder to have unfettered access to Defendant's entire network.

26. Once inside Defendant's system, the intruder used privileged access to explore the Command platform, Defendant's web-based customer platform. Defendant's personnel can remotely access customer camera feeds via the Command platform in order to provide technical support, view customers' live camera feeds (which may include captures of consumers), and access stored personal identifying information (such as archived video footage and still images, and anything visible therein).

27. Through the Command platform, the intruder had access to over 150,000 live customer cameras and viewed patients in psychiatric hospitals (including patients resting in hospital beds) and women's health clinics, young children playing inside of a room, and incarcerated persons inside of their cells.

28. After hours of exploration into Defendant's customer support server and security camera feeds, the intruder self-reported the breach to the news media. Defendant remained unaware of the breach until a media outlet contacted Defendant for comment.

29. Defendant's internal investigation determined that the threat actor:

a. Accessed thousands of customer cameras—some of which were viewed for upwards of 90 minutes;

b. Exfiltrated several gigabytes of data containing customers' and consumers' information, including: (1) names, (2) email addresses, (3) physical addresses, (4) customer usernames and password hashes, (5) live camera footage, (6) video archives, (7) still images, (8) persons/vehicles of interest, (9) location maps and geolocation data for devices placed on maps, (10) customers' site floorplans, (11) audit log data and product utilization analytics, (12) license status, (13) user permissions and roles, (14) audio recordings, (15) names and titles of organization contacts, and (16) customer Wi-Fi credentials;

c. Performed searches using Defendant's "People Analytics" feature; and

d. Executed remote shell commands (e.g., executing commands from a remote machine) to customers' security cameras.

30. Even after the March 2021 breach and Defendant's remediation efforts, Defendant's information security program still posed serious risks to customers' and consumers' personal information. Following the breach, in July 2021, a third-party security assessor reviewed Defendant's general information security practices and Defendant's security as it relates to the Command platform and uncovered a set of common application flaws. According to the assessor's evaluation, significant deficiencies included:

a. A lack of authorization controls on a NetSuite subdomain endpoint allowed non-privileged users to access sales order data containing sensitive customer information; and

b. Incorrect authorization checks on a hyperzoom API endpoint allowed attackers to retrieve video belonging to other organizations without authorization.

DEFENDANT'S INFORMATION SECURITY FAILURES HARMED CONSUMERS

31. Defendant's failure to provide reasonable security for customers' and consumers' personal information has caused or is likely to cause substantial injury to customers and consumers.

32. Customers have suffered or are likely to suffer substantial injury in the form of increased exposure to fraud and identity theft, leading to monetary loss and time spent remedying the problem. Information exfiltrated from Defendant's network included customers' names, email addresses, physical addresses, usernames and password hashes, live camera footage, video archives, still images, person/vehicles of interest to the customer, location maps and geolocation data for devices placed on maps, customers' site floorplans, audit log data and product utilization analytics, license status, user permissions and roles, audio recordings, names and titles of organization contacts, and customer Wi-Fi credentials.

33. Since the breach, customers have reported increased phishing attempts seeking personal information, putting customers and consumers at higher risk for injury in the future. Malicious actors combine personal information to perpetrate fraud (for example, by opening fraudulent lines of credit) or obtain additional personal information by impersonating companies with whom the target has previously transacted.

34. Consumers have suffered or are likely to suffer substantial injury in the form of exposure of their personal information and by the invasion of their privacy as result of unauthorized surveillance of consumers in sensitive settings such as hospital rooms and schools. Information exfiltrated about consumers from Defendant's network included live camera footage, video archive, still images, and persons/vehicles of interest.

35. These harms, described in Paragraphs 32-34, were not reasonably avoidable by customers or consumers. Defendant's customers had no way of independently knowing about Defendant's security failures. In fact, everything presented by Defendant to customers suggested that Defendant took data security very seriously and implemented safeguards to protect customers' and consumers' personal

information—which was not the case. Moreover, most consumers did not know, and could not have known, that Defendant's security cameras were even in use in places they visited.

36. Further, the harms are not outweighed by any countervailing benefits. Defendant could have prevented or mitigated these information security failures through well known, readily available, and relatively low-cost measures. For example, Defendant could have, among other things: (1) trained engineers and developers on industry best practices for configuration updates; (2) scanned code repositories for unsecured credentials; (3) developed access management practices using the principle of least privilege to ensure that the minimal amount of accounts had privileged access; (4) implemented a data loss prevention solution for high priority servers, such as the customer service server, to ensure that actions such as the creation, deletion, and exfiltration of files created alerts; or (5) developed centralized logging and alerting capabilities to respond to suspicious activity in a timely fashion. Any of these measures would have either prevented or minimized the impact of the March 2021 breach.

DEFENDANT'S INFORMATION SECURITY MISREPRESENTATIONS

37. Defendant made representations about its information security practices that were false and misleading.

38. Since 2018 Defendant's privacy policy has claimed that "[a]t Verkada, we take customer privacy seriously" and "[w]e will use best-in-class data security tools and best practices to keep your data safe and protect the Verkada Products from unauthorized access." Defendant's privacy policy also stated that it "use[s] industry-standard methods to keep [customers'] information safe and secure while it is transmitted over your local area network and through the Internet to our servers."

39. Also since 2018, through its "Trust" webpage, Defendant has made numerous claims regarding Defendant's information security practices. For instance, until at least 2021, Defendant stated that "[f]rom Day 1, we've made technology decisions that strengthen security and…Verkada uses commercially reasonable efforts to deploy and uphold [] security best practices and standards…."

40. Since its inception, Defendant has touted its products as being the secure option for customers seeking video surveillance systems. In an April 2018 press release, Defendant declared "[a]s a challenger in the $16 billion-a-year market for commercial video surveillance technology, Verkada

offers a range of benefits, including stronger data security…." Defendant further reassured customers, since at least August 2018, that "Verkada replaces obsolete equipment with technology that's smart, secure, and easy to manage." In an October 2018 blog post, Defendant stated that "Verkada's hybrid cloud solution…takes serious precautions to lower the chance of a data breach." In this same blog post, Defendant assured that with its "hybrid cloud solution, the burden of staying compliant is partially offloaded to your security vendor. The vendor becomes responsible for making sure the system stays aligned with security, storage, and accessibility standards (such as HIPAA, PCI compliance and the latest vulnerabilities)…."

41. Defendant discussed specific risks to cloud security cameras, including Mirai malware, in a June 2019 article. Defendant claimed that "cybersecurity for surveillance cameras must be an utmost priority for end users in 2019. Any organization that has failed to properly safeguard its camera solution should see this as a wake-up call." Defendant also stated that "[f]rom day 1, we designed Verkada with network security in mind," and provided examples as to "[h]ow Verkada [p]rioritizes [c]ybersecurity." For example, Defendant claimed "[w]e implement regular penetration testing conducted by independent third parties to ensure that there are no undiscovered exploits."

42. In a January 2020 interview, Defendant's CEO stated: "We built a system that's end-to-end secure. That's a huge problem with today's systems. Verkada is secure out of the box."

43. Moreover, since at least March 2020, Defendant has posted on its website its data security statement. Among other things, the data security statement included the following claims regarding the strength of Defendant's information security practices:

> **Secure by Default.** Verkada's solution is secure out of the box, featuring end-to-end encryption....
>
> **Introduction.** Security was top of mind when designing Verkada. That's why we redesigned video security infrastructure [] and built a system that's secure from the ground up....
>
> **Hardware Security.** At Verkada, cybersecurity isn't a last minute addition. We build our devices from the very first step....

> **Network Security** ... At Verkada, we pull out all the stops to ensure that your data is protected as it's transmitted over the network....
>
> **Encryption in Transit.** We encrypt all data that is sent over the network with AES 128 standards. On top of that, we exclusively use HTTPS over TLS v1.2 to add an extra layer of security. Encryption means any malicious interception (be it MITM or Eavesdropping) is neither fatal nor compromising...bad actors are unable to push malware directly onto our devices.
>
> **Application Security.** Security starts with us … Verkada gives you the tools you need to control who has access to your system, and what they do with that access....
>
> **Regular Penetration Testing.** We employ an independent security firm to continually run penetration tests on our systems. This is how we find and fix security exploits before they ever threaten our customers.

44. In a March 2020 article, Defendant acknowledged that data collected by video security cameras and internet enabled devices is "often sensitive," and that "Network Security is one of the most critical spaces to keep secure, especially for a 24/7 cloud-connected model like Verkada's…." Defendant then claimed that "its commitment to a comprehensively secure surveillance environment has not changed" and that it "focus[es] on security measures" and "protect[ing] your data during transit and at rest in the cloud."

45. An article published by Defendant around September 2020 stated that "Verkada's systems are purposefully designed to minimize the attack surface that could be exploited by malicious actors …. This system architecture eliminates a number of insecure components, practices, and protocols that are common with competing technology…."

46. Defendant has routinely represented that customers' data is protected using "encryption in transit and at rest." For example, Defendant's "Encryption and Security" article on its website claims that "Verkada's modern system architecture and security infrastructure ensures that there is end-to-end

encryption," and that it uses "[e]nd to end state-of-the-art AES encryption, ensuring the security of data in storage and in transit."

47. Defendant also made specific security statements regarding the Command platform on its website. For example:

> **Top Security Features by Verkada in 2020**. With Command, our cloud-based management platform, we're able to quickly develop and roll out new security features and enhancements—automatically, and at no cost—ensuring that end users have the best technology to protect people, assets, and privacy.

DEFENDANT'S DECEPTIVE HIPAA REPRESENTATIONS

48. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191, is a statute that sets forth privacy and information security protections for certain consumer health information.

49. Defendant is a Business Associate under HIPAA in that it, "[o]n behalf of [a] covered entity[,]… creates, receives, maintains, or transmits protected health information for a function or activity … including … data analysis … [and] patient safety activities…." 45 C.F.R. § 160.103. As a Business Associate, Defendant is required to comply with the HIPAA Security Rule. *See* Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 U.S.C. § 17931.

50. Defendant has publicly claimed HIPAA certification or compliance on several occasions since at least 2019. For example, on August 22, 2019, Defendant posted an article on its website titled, "Security At Scale," wherein Defendant's CEO stated, "health care is an emerging segment for us because we are conscious enough about privacy to be compliant with HIPAA."

51. Since at least March 2020, Defendant has told healthcare providers on its website that it can "[i]mprove safety across healthcare facilities with Verkada's HIPAA compliant solution." On the same page, Defendant also says that "Verkada's HIPAA compliant video security solution allows healthcare practitioners to easily manage site and patient safety – in a secure and scalable way," encouraging prospective customers to "[d]iscover why hospitals and healthcare facilities choose

Verkada's HIPAA compliant solution," and assuring prospective customers that "Verkada's HIPAA compliant system is secure by default."

52. In a press release issued in April 2020, at the beginning of the COVID-19 pandemic, Defendant proclaimed that: "Over 200 leading healthcare providers already use Verkada's HIPAA compliant video solution. With a focus on customer privacy and security, Verkada provides customers with the tools to ensure patients and staff are always protected."

53. Moreover, between at least July 2020 to April 2021, on the "Compliance & Security Regulations" section of its "Secure by Default" webpage, Defendant claimed that "Verkada devices are certified against some of the strictest data handling and security standards in the world," and list HIPAA as the first standard. Since then, Defendant has claimed that "Verkada devices are compliant against some of the strictest data handling and security standards in the world" and continue to prominently display its purported HIPAA compliance. Between at least November 2020 to April 2021, in Defendant's help article entitled "Verkada Compliance Info," Defendant claimed that "Verkada cameras are certified for … HIPAA … compliance."

54. Moreover, Defendant relayed that it is "[f]ully HIPAA compliant" to prospective customers in marketing emails, encouraging prospective customers to attend webinars to learn how "leading healthcare organizations are deploying HIPAA compliant cameras in just minutes." Defendant amplified this messaging during the COVID-19 pandemic, informing prospective customers in marketing emails that "[w]ith this challenge and Verkada in mind, we designed Verkada's HIPAA compliant video security solution …."

55. A "Security Posture Assessment" conducted by a third party in February 2021 concluded that, "[w]hile policies and controls and procedures seem to have been implemented for HIPAA[,]…evidence of compliance with [this] framework could not be located and no holistic framework-based security program has been fully implemented."

56. As discussed above in Paragraph 20, Defendant has engaged in multiple practices that, taken individually or together, failed to provide reasonable or appropriate security for the personal information, including protected health information, that it collected and maintained about consumers.

57. Following the March 2021 breach, several customers expressed frustration regarding Defendant's purported HIPAA compliance. One customer stated: "I think a reasonable person believes that a 3rd party has done an actual certification…." Another customer stated: "I've been told on a number of occasions that you were HIPAA compliant. This breach verified that is not the case…."

DEFENDANT'S DECEPTIVE PRIVACY SHIELD COMPLIANCE REPRESENTATION

58. The Department of Commerce ("Commerce") and the European Commission negotiated the Privacy Shield to provide a mechanism for companies to transfer personal data from the European Union to the United States in a manner consistent with the requirements of European Union law on data protection. The Swiss-U.S. Privacy Shield framework is identical to the EU-U.S. Privacy Shield framework.

59. Privacy Shield expressly provides that, while decisions by organizations to "enter the Privacy Shield are entirely voluntary, effective compliance is compulsory: organizations that self-certify to [Commerce] and publicly declare their commitment to adhere to the Principles must comply fully with the Principles."

60. The Privacy Shield Principles include the following:

> SECURITY [Principle 4]: (a) Organizations creating, maintaining, using, or disseminating personal information must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

61. To join the EU-U.S. and/or Swiss-U.S. Privacy Shield framework, a company would self-certify its compliance with the Privacy Shield Principles to Commerce and annually re-certify its compliance.

62. Under both frameworks, for companies that claim to have self-certified to the Privacy Shield Principles, failure to comply or otherwise to "fully implement" the Privacy Shield Principles "is enforceable under Section 5 of the Federal Trade Commission Act."

63. From at least November 2018 until November 2020, Defendant maintained a self-certification.

64. From at least September 2018 to December 2020 Defendant's Privacy Statement stated that "Verkada complies with the EU-US and Swiss-US Privacy Shield Frameworks … regarding the collection, use, and retention of personal information from European Union member countries and Switzerland, respectively…."

65. Until at least December 2022, Defendant claimed on its "Global Operations" web page that "Verkada has achieved Privacy Shield certification for international data transfers."

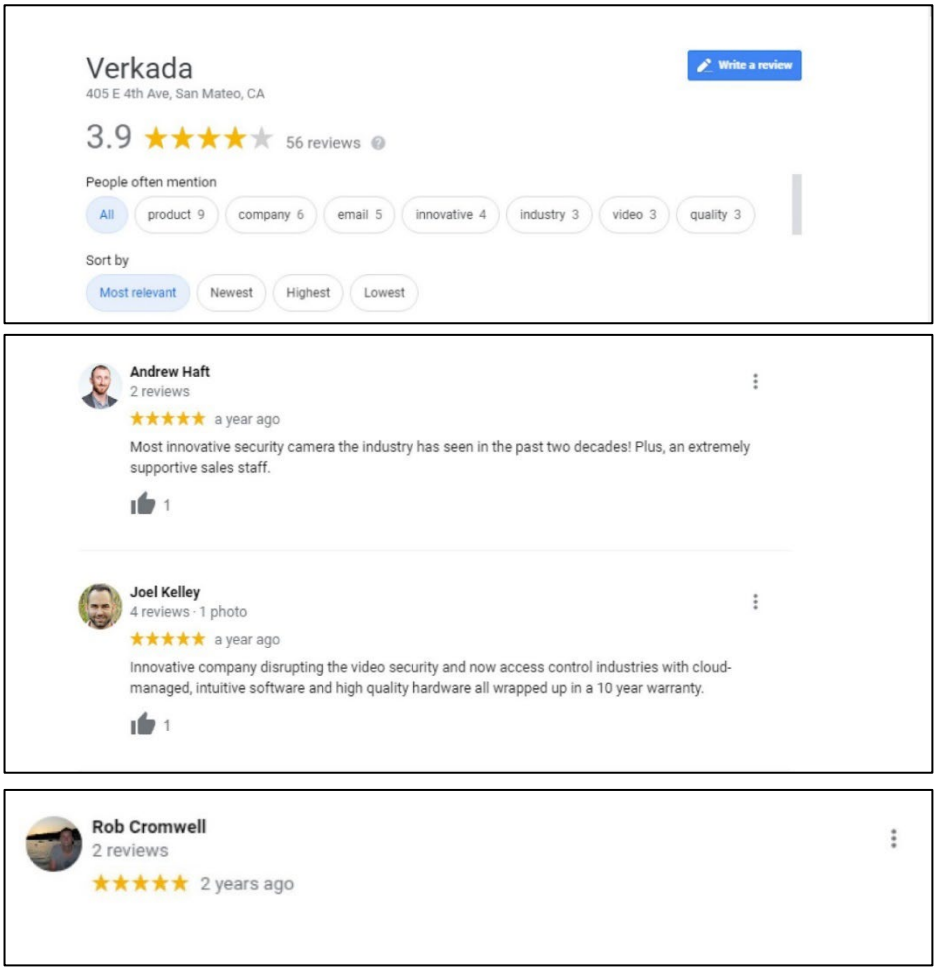
66. In numerous marketing emails, Defendant informed prospective customers that it was "Privacy Shield Certified."

67. As described above in Paragraph 20, Defendant failed to take reasonable and appropriate security measures to protect consumers' personal information.

68. Although the European Court of Justice determined on July 16, 2020 that the EU-U.S. Privacy Shield framework was not adequate for allowing the lawful transfer of personal data from the European Union and the Swiss Data Protection and Information Commissioner determined on September 8, 2020 that the Swiss-U.S. Privacy Shield framework was similarly inadequate, those decisions do not change the fact that Defendant represented to consumers that it was certified under both Privacy Shield frameworks, and as such, would fully comply with the Principles, including Principle 4. Nor does it change the fact that, at times, Defendant represented that it was Privacy Shield certified when, in fact, it was not.

DEFENDANT'S FALSE AND MISLEADING ONLINE RATINGS AND REVIEWS

69. On multiple occasions beginning in or around October 2019, Defendant's employees, as well as a venture capitalist who invested in Defendant ("venture capital investor"), posted positive ratings and reviews of Defendant and its products on Google Maps and failed to disclose their association or current employment status with the company. For example, the Vice President of Engineering (Rob Cromwell), an Account Executive (Andrew Haft), and an Engineer (Joel Kelly) all posted 5-star ratings and reviews:



70. Indeed, Defendant encouraged at least some employees to post a review or rating in early 2020.

71. As of June 2023, almost 35% of Defendant's Google Maps ratings and reviews were posted by Defendant's employees or a venture capital investor.

72. Defendant was aware of these ratings and reviews by its employees and the venture capital investor and still failed to disclose their association with Defendant. In fact, since Defendant became aware of the Commission's investigation, more than ten additional positive ratings and reviews have been posted by individuals associated with Defendant.

DEFENDANT'S FAILURES WITH RESPECT TO COMMERCIAL ELECTRONIC MAIL

73. Defendant relies on commercial email campaigns as a means of promoting Defendant's products and services, which are commercial in nature. Defendant's sales and marketing teams manage

such campaigns. Defendant's reliance on these campaigns has grown exponentially, sending more than 2 million commercial email messages in 2019, more than 6 million in 2020, and more than 22 million in 2021. Additionally, multiple email messages were sent to the same recipients.

74. Numerous recipients complained about Defendant's incessant commercial emails. Among other things, recipients have repeatedly notified Defendant that the emails are unwanted marketing communications and that they are unable to unsubscribe from these emails despite substantial efforts.

75. Defendant's commercial email messages do not consistently include a valid physical postal address.

76. Defendant does not include clear and conspicuous notice of the opportunity to opt-out in its commercial email messages.

77. Even if a recipient requests to opt-out of receiving emails, Defendant fails to honor recipients' requests to opt out from promotional messages within ten business days of such requests and routinely ignores requests to stop receiving Defendant's promotional messages.

78. Based on the facts and violations of law alleged in this Complaint, the FTC has reason to believe that Defendant is violating or is about to violate laws enforced by the Commission because, among other things, Defendant only examined its conduct after it was either made aware of the data security breaches or was under investigation.

VIOLATIONS OF THE FTC ACT

79. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

80. Misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices prohibited by Section 5(a) of the FTC Act.

81. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

Count I – Unfair Information Security Practices (Business Customers)

82. In numerous instances, Defendant has failed to take reasonable steps to prevent unauthorized access to customers' personal information on its network and customer cameras.

83. Defendant's acts or practices cause or are likely to cause substantial injury to customers that customers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

84. Therefore, Defendant's acts or practices as described in Paragraph 82 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. §§ 45(a), (n).

Count II – Unfair Information Security Practices (Consumers)

85. In numerous instances, Defendant has failed to take reasonable steps to prevent unauthorized access to consumers' personal information, including video footage of consumers at sensitive locations, on its network and customer cameras.

86. Defendant's acts or practices cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

87. Therefore, Defendant's acts or practices as described in Paragraph 85 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. §§ 45(a), (n).

Count III – Information Security Misrepresentations

88. In numerous instances in connection with the advertising, marketing, promotion, offering for sale, or sale of security cameras, Defendant represents, directly or indirectly, expressly or by implication, that it uses appropriate safeguards to protect customers' and consumers' personal information collected through Defendant's security cameras.

89. In fact, in numerous instances in which Defendant has made the representations described in Paragraph 88, Defendant does not use appropriate safeguards to protect customers' and consumers' personal information collected through Defendant's security cameras.

90. Therefore, Defendant's representations as described in Paragraph 88 are false or misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count IV – Information Security Misrepresentations—Command Platform

91. In numerous instances in connection with the advertising, marketing, promotion, offering for sale, or sale of security cameras, Defendant represents, directly or indirectly, expressly or by implication, that it uses appropriate safeguards to protect customers' and consumers' personal information on the Command platform.

92. In fact, in numerous instances in which Defendant has made the representations described in Paragraph 91, Defendant does not use appropriate safeguards to protect customers' and consumers' personal information on the Command platform.

93. Therefore, Defendant's representations as described in Paragraph 91 are false or misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count V – HIPAA Misrepresentations

94. In numerous instances in connection with the advertising, marketing, promotion, offering for sale, or sale of security cameras, Defendant represents, directly or indirectly, expressly or by implication, that Defendant's security camera systems are HIPAA certified or compliant.

95. In fact, despite numerous instances in which Defendant has made the representations described in Paragraph 94, Defendant's security camera systems are not HIPAA certified or compliant.

96. Therefore, Defendant's representations as described in Paragraph 94 are false or misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count VI – Privacy Shield Compliance Misrepresentations

97. In numerous instances in connection with the advertising, marketing, promotion, offering for sale, or sale of security cameras, Defendant has represented, directly or indirectly, expressly or by

implication, that Defendant adhered to the EU-U.S. and Swiss-U.S. Privacy Shield principles, including the principle of security.

98. In fact, in numerous instances in which Defendant has made the representations described in Paragraph 97, Defendant did not adhere to the EU-U.S. and Swiss-U.S. Privacy Shield principles, including the principle of security.

99. Therefore, Defendant's representations as set forth in Paragraph 97 are false or misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count VII – False Claim of Impartial Ratings and Reviews

100. In numerous instances in connection with the advertising, marketing, promotion, offering for sale, or sale of security cameras, Defendant represents, directly or indirectly, expressly or by implication, that online, consumer ratings and reviews of Verkada or its products reflect the experiences or opinions of ordinary, impartial customers.

101. In fact, in numerous instances in which Defendant has made the representations described in Paragraph 100, these online consumer ratings and reviews of Verkada or its products do not reflect the experiences or opinions of ordinary impartial customers, but instead were written by Verkada employees or a venture capital investor.

102. Therefore, Defendant's representations described in Paragraph 100 are false or misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a)

Count VIII – Deceptive Failure to Disclose Material Connections

103. In numerous instances in connection with the advertising, marketing, promotion, offering for sale, or sale of security cameras, Defendant represents, directly or indirectly, expressly or by implication, that online consumer ratings and reviews of Verkada or its products posted on Google Maps reflect its customers' opinions or experiences.

104. In numerous instances in which Defendant makes the representation described in Paragraph 103, Defendant has failed to disclose to consumers that the online consumer ratings and

reviews of Verkada or its products were written by Verkada employees or a venture capital investor. This additional information would be material to consumers in evaluating the reviews in connection with a purchase or use decision.

105. In light of the representations described in Paragraph 103, Defendant's failure to disclose the material information as described in Paragraph 104, constitutes a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

VIOLATIONS OF THE CAN-SPAM ACT

106. The CAN-SPAM Act became effective on January 1, 2004, and has since remained in full force and effect.

107. Section 3(2)(A) of the CAN-SPAM Act states that a "commercial electronic mail message" is "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)." 15 U.S.C. § 7702(2)(A).

108. Section 3(9) of the CAN-SPAM Act states, in pertinent part, that "[t]he term 'initiate,' when used with respect to a commercial electronic mail message, means to originate or transmit such message or to procure the origination or transmission of such message…." 15 U.S.C. § 7702(9).

109. Section 3(13) of the CAN-SPAM Act states that "[t]he term 'protected computer' has the meaning given that term in section 1030(e)(2)(B) of Title 18." 15 U.S.C. § 7702(13). Section 1030(e)(2)(B) of Title 18 states that "[t]he term 'protected computer' means a computer … which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B).

110. Section 5(a)(4)(A) states: "If a recipient makes a request using a mechanism provided … not to receive some or any commercial electronic mail messages from such sender, then it is unlawful—(i) for the sender to initiate the transmission to the recipient, more than 10 business days after the receipt of such request, of a commercial electronic mail message that falls within the scope of the request…" 15 U.S.C. § 7704(a)(4)(A).

111. Section 5(a)(5)(A) of the CAN-SPAM Act states: "It is unlawful for any person to initiate the transmission of any commercial electronic mail message to a protected computer unless the message provides—… (ii) clear and conspicuous notice of the opportunity under paragraph (3) to decline to receive further commercial electronic mail messages from the sender; and…" (iii) a valid physical postal address of the sender." 15 U.S.C. § 7704(a)(5)(A).

112. Section 7(e) of the CAN-SPAM Act, 15 U.S.C. § 7706 (e), states that in any action to enforce compliance with Section 5(a)(4)(A) and other specified sections of CAN-SPAM through an injunction, the FTC need not allege or prove the state of mind required by such sections.

113. Pursuant to Section 7(a) of the CAN-SPAM Act, 15 U.S.C. § 7706(a), a violation of the CAN-SPAM Act is treated as a violation of a rule promulgated under the FTC Act regarding unfair or deceptive acts or practices.

114. Pursuant to Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the CAN-SPAM Act constitutes an unfair or deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count IX – Failure to Honor Opt-Out Requests

115. In numerous instances, Defendant initiates the transmission, to protected computers, of commercial electronic mail messages to a recipient more than ten business days after the receipt of a request not to receive further commercial electronic mail messages from Defendant at the recipient's email address.

116. Therefore, Defendant's acts or practices as described in Paragraph 115 violate Section 5(a)(4)(A) of the CAN-SPAM Act, 15 U.S.C. § 7704(a)(4)(A), and Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count X – Failure to Provide Notice of Opt-Out

117. In numerous instances, Defendant initiates the transmission, to protected computers, of commercial electronic mail messages that do not provide a clear and conspicuous notice of the opportunity under 15 U.S.C. § 7704(a)(3) to decline to receive further commercial electronic mail messages from Defendant.

118. Therefore, Defendant's acts or practices as described in Paragraph 117 violate 5(a)(5)(A)(ii) of the CAN-SPAM Act, 15 U.S.C. § 7704(a)(5)(A)(ii), and Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count XI – Failure to Provide Valid Physical Postal Address

119. In numerous instances, Defendant initiates the transmission, to protected computers, of commercial electronic mail messages that do not provide a valid physical postal address of Defendant.

120. Therefore, Defendant's acts or practices, as described in Paragraph 119 violate Section 5(a)(5)(A)(iii) of the CAN-SPAM Act, 15 U.S.C. § 7704(a)(5)(A)(iii), and Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

CONSUMER INJURY

121. Consumers are suffering, have suffered, and will continue to suffer substantial injury as a result of Defendant's violations of the FTC Act and the CAN-SPAM Act. Absent injunctive relief by this Court, Defendant is likely to continue to injure consumers and harm the public interest.

CIVIL PENALTIES

122. Section 5(m)(1) of the FTC Act, 15 U.S.C. § 45(m)(1)(A), authorizes this Court to award civil penalties for each violation of the CAN-SPAM Act.

123. Defendant violated the CAN-SPAM Act with the knowledge required by Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A).

PRAYER FOR RELIEF

124. Wherefore, Plaintiff requests that the Court:

a. Enter a permanent injunction to prevent future violations of the FTC Act and the CAN-SPAM Act;

b. Impose civil penalties for each violation of the CAN-SPAM Act; and

c. Award any additional relief as the Court determines to be just and proper.

Dated: August 30, 2024

FOR PLAINTIFF THE UNITED STATES OF AMERICA:

ISMAIL J. RAMSEY
United States Attorney
Northern District of California

/s/ Vivian F. Wang
VIVIAN F. WANG
Assistant United States Attorney
United States Attorney's Office
for the Northern District of California
Phone: (415) 436-7134
vivian.wang@usdoj.gov

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General
BURDEN H. WALKER
Acting Deputy Assistant Attorney General
Civil Division

AMANDA N. LISKAMM
Director
LISA K. HSIAO
Senior Deputy Director, Civil Litigation
ZACHARY A. DIETERT
Assistant Director

/s/ Cameron A. Brown
CAMERON A. BROWN
AMANDA K. KELLY
Trial Attorneys
JAMES T. NELSON
Senior Trial Attorney
Consumer Protection Branch
U.S. Department of Justice
450 5th Street, N.W.
Sixth Floor, South
Washington, D.C. 20001
(202) 514-9471
Cameron.A.Brown@usdoj.gov

Of Counsel:

BENJAMIN WISEMAN
Associate Director
Division of Privacy and Identity Protection

TIFFANY GEORGE
Assistant Director
Division of Privacy and Identity Protection

JACQUELINE K. FORD
Attorney
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
(202) 326-2844 (voice)
(202) 326-3062 (fax)

KAMAY LAFALAISE
Attorney
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
(202) 326-3780 (voice)
(202) 326-3062 (fax)